

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-242224

(43)Date of publication of application : 17.09.1996

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

G09C 1/00

(21)Application number : 07-044515

(71)Applicant : MEYA TATSUHIRO

(22)Date of filing : 03.03.1995

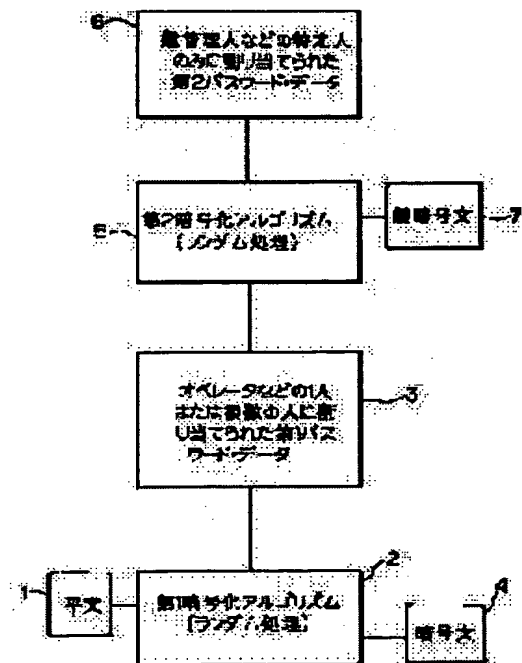
(72)Inventor : MEYA TATSUHIRO

(54) METHOD FOR CONSTRUCTING SECURITY

(57)Abstract:

PURPOSE: To construct highly advanced security.

CONSTITUTION: First prescribed ciphering algorithm 2 is applied to the data of a normal sentence 1 and a ciphered sentence 4 is generated from the normal sentence 1 by executing randomizing processing based upon 1st pass word data 3 allocated to one or plural persons. On the other hand, randomizing processing is executed once or more by the use of 2nd prescribed ciphering algorithm 5 which is the same or different as/from the 1st ciphering algorithm 2 based upon 2nd pass word data 6 allocated only to a specific custodian or the like as data inherent in the specific person to generate a key ciphered sentence 7 from the data 3 and the ciphered sentence 7 is stored and managed by the specific custodian or the like.



LEGAL STATUS

[Date of request for examination] 03.03.1995

[Date of sending the examiner's decision of rejection] 31.03.1999

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 11-07253

[Date of requesting appeal against examiner's decision of rejection] 28.04.1999

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-242224

(43) 公開日 平成8年(1996)9月17日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00			H 0 4 L 9/00	Z
	9/10	7259-5 J	G 0 9 C 1/00	
	9/12			
G 0 9 C 1/00				

審査請求 有 請求項の数 5 O L (全 5 頁)

(21) 出願番号 特願平7-44515

(22) 出願日 平成7年(1995)3月3日

(71) 出願人 595032185

女屋 遼賢

東京都町田市原町田3-7-10 ハイコー
ト矢口301

(72) 発明者 女屋 遼賢

東京都町田市原町田3-7-10 ハイコー
ト矢口301

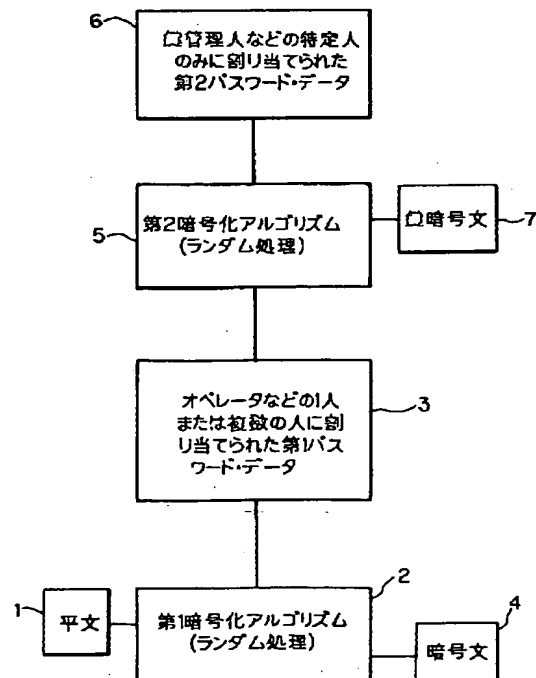
(74) 代理人 弁理士 萩野 平 (外5名)

(54) 【発明の名称】 セキュリティ構築方法

(57) 【要約】

【目的】 より高度なセキュリティを構築することができるセキュリティ構築方法を提供することを目的とする。

【構成】 平文1のデータに対して所定の第1暗号化アルゴリズム2を使用して1人または複数の人に割り当てられた第1パスワード・データ3によりランダム化処理を行って平文1から暗号文4を生成する。また、特定の管理人などにのみ割り当てられた特定人固有の第2パスワード・データ6により、第1暗号化アルゴリズム2と同じかまたは異なる所定の第2暗号化アルゴリズム5を使用して1回以上のランダム化処理を行って、第1パスワード・データ3から鍵暗号文7を生成し、鍵暗号文7を特定の管理人などにより保管管理を行う。



【特許請求の範囲】

【請求項 1】 所定の暗号化アルゴリズムを使用し、第 1 のパスワードデータを鍵として平文データをランダム処理し、前記平文から暗号文を生成する工程と、特定人に割り当てられた固有の第 2 のパスワードデータを鍵として、前記暗号化アルゴリズムあるいはそれとは異なる所定の暗号化アルゴリズムを使用して前記第 1 のパスワードデータをランダム処理し、前記第 1 のパスワードデータから鍵暗号文を生成する工程と、からなるセキュリティ構築方法。

【請求項 2】 前段工程で使用したパスワードデータを、前記各暗号化アルゴリズムの何れかあるいはそれらとは異なる所定の暗号化アルゴリズムを使用してランダム処理し、前段工程で使用したパスワードデータから鍵暗号文を生成する工程を繰り返し実行する請求項 2 に記載のセキュリティ構築方法。

【請求項 3】 前記第 2 のパスワードデータが、少なくとも 1 つの固有情報を有することを特徴とする請求項 1 若しくは 2 に記載のセキュリティ構築方法。

【請求項 4】 前記第 2 のパスワードデータが、装置自体に割り当てられた固有情報を有することを特徴とする請求項 3 に記載のセキュリティ構築方法。

【請求項 5】 前記第 2 のパスワードデータが、特定人に割り当てられた固有情報であることを特徴とする請求項 3 に記載のセキュリティ構築方法。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 本発明は、例えば、パーソナルコンピュータ（以下、パソコンと略称する）などのソフトウェアの不法複製、データ通信などに供するデータの秘匿性の保護、秘密データの改ざん防止などに有効なセキュリティ構築方法に関する。

【0002】

【従来の技術】 近似、パソコンの急速な普及に伴い、パソコン通信も盛んになり、コンピュータウイルスのパソコンへの侵入のみならず、秘密伝送データのコンピュータハッカによる破壊、秘密データの改ざん、さらには、パソコン通信に限らずソフトウェアの不法複製による知的所有権の侵害などが行われる可能性が高まってきている。このようなデータの破壊やデータの不法複製、データの改ざんなどを防止すべく、従来より種々のセキュリティ対策が講じられている。この一例として、データの改ざんが行われないように、また、通信データの機密漏洩が防止されるように、平文（誰が読んでも理解できる文書）のデータの暗号化を行って、暗号文（何らかの手段を施して翻訳しなければ、読めない文章）を生成する方法が採られている。

【0003】 このデータの暗号化に際して、データのブロック暗号が主流をなしており、ブロック暗号化のあるアルゴリズムを公開しているものとして、例えば、DE

S (Data Encryption Standard: データ暗号化規格) と FEAL (Fast Data Encipherment Algorithm: 高速データ暗号化アルゴリズム) と呼ばれる暗号化アルゴリズムがある。

【0004】 DES 及び FEAL は、暗号化アルゴリズムを公開したアルゴリズム公開型暗号化法であり、暗号化に際して秘密鍵と称されるパスワードデータを用いている。

【0005】

【発明が解決しようとする課題】 上述のように、データの暗号化に際して、従来から種々の暗号化アルゴリズムが利用されている。DES 及び FEAL は、秘密鍵を用いた公開型暗号化法であるが秘密鍵の管理が万全でなければ、秘密鍵が不特定人に知られてしまい、容易に暗号文が解読されてしまう。データのセキュリティを構築する場合、不特定多数のオペレータがパソコンを使用し、秘匿性を保持すべきデータをパソコンのディスクファイルに保管しておくような場合には、データが上述のように暗号化されいても、不特定多数のオペレータの中に鍵を入手できる者がいれば、暗号文を解読することができる。このように、データのセキュリティを構築する場合、暗号化アルゴリズムを強化することは勿論のこと、データの暗号化のための秘密鍵の管理を重視して初めて、システム全体の安全なセキュリティが構築される。

【0006】 本発明は、上記事情に鑑みなされたものであり、より高度なセキュリティを構築することができるセキュリティ構築方法を提供することを目的とする。

【0007】

【課題を解決するための手段】 上記目的を達成するために、本発明は、所定の暗号化アルゴリズムを使用し、第 1 のパスワードデータを鍵として平文データをランダム処理し、前記平文から暗号文を生成する工程と、特定人に割り当てられた固有の第 2 のパスワードデータを鍵として、前記暗号化アルゴリズムあるいはそれとは異なる所定の暗号化アルゴリズムを使用して前記第 1 のパスワードデータをランダム処理し、前記第 1 のパスワードデータから鍵暗号文を生成する工程とからなる。さらに、前段工程で使用したパスワードデータを、前記各暗号化アルゴリズムの何れかあるいはそれらとは異なる所定の暗号化アルゴリズムを使用してランダム処理し、前段工程で使用したパスワードデータから鍵暗号文を生成する工程を繰り返し実行するものである。さらに、前記第 2 のパスワードデータが、少なくとも 1 つの固有情報から成るものである。さらに、前記第 2 のパスワードデータが、装置自体に割り当てられた固有情報を有するものである。若しくは、前記第 2 のパスワードデータが、特定人に割り当てられた固有情報である。

【0008】

【作用】 上記構成によれば、平文のデータを所定の暗号化アルゴリズムを使用して所定の人に割り当てられた第

1パスワードデータによりランダム化処理を行い、平文のデータから暗号文を生成する。さらに、暗号文生成時に使用したのと同じ暗号化アルゴリズムあるいはそれとは異なる暗号化アルゴリズムを使用して第1パスワードデータを特定人のみに割り当てられた特定人固有の第2パスワードデータによりランダム化処理を実行して、第1パスワードデータから鍵暗号文を生成し、平文の暗号文に対する鍵を第1、第2パスワードデータによるランダム化処理で2重の暗号化を行うことにより、暗号文の解読をより一層難解なものにするとともに、システム全体が固有の情報でのみ有効な働きをするシステムセキュリティが成立する。鍵のランダム化処理は、必要に応じて多数回実行することができる。例えば、前工程で使用したパスワードデータを第3パスワードデータによりランダム化処理を実行して新たな鍵暗号文を生成することにより、平文の暗号文に対する鍵を第1、第2さらに第3パスワードデータによるランダム化処理で多重の暗号化を実行することができる。

【0009】

【実施例】以下、本発明のセキュリティ構築方法の実施例について図面に基づき説明する。図1はその一実施例を説明するための暗号文作成のための処理手順を示す説明図である。図1における1は、平文であり、この平文1は、例えばパソコン通信などに供するものである。この平文1のデータを伝送するに際し、あるいは任意に使用するのに、データの秘匿性を保持するために、まず、平文1のデータの暗号化を行う。このデータの暗号化を行うには、従来より公知のDESまたはFEALに使用される暗号化アルゴリズム、あるいはその他の任意のデータの暗号化アルゴリズム2（以下、第1暗号化アルゴリズムという）を使用して、例えば、1人あるいは特定された複数のパソコンオペレータなどに割り当てられ、これらの1人あるいは特定された複数のパソコンオペレータなどのみが知り得るパスワードデータ3（以下、第1パスワードデータという）によりランダム化処理を行って暗号文4を生成する。この暗号文4は、パソコン通信を行う場合には、通信回線を通して伝送したり、あるいは所定のデータの解析用などに使用したりされる。

【0010】このようにして得れた暗号文4は、例えば、前記の1人または複数のパソコンオペレータなど以外は解読できないように、暗号文4のために、鍵管理を行う。この鍵管理に際して、本実施例では、前記第1のパスワードデータ3に対して前記第1暗号化アルゴリズム2またはこの第1暗号化アルゴリズム2とは異なる任意の暗号化アルゴリズム5（以下、これらを含めて第2暗号化アルゴリズムという）を使用して鍵管理人や、企業の経営者などの特定の人のみに割り当てられた特定人固有のパスワードデータ（以下、第2パスワードデータという）6によりランダム化処理を行うことにより、鍵暗号文7を生成する。

【0011】このランダム暗号化処理は、1回でもよいが、複数回行うことにより、鍵がより高い階層に存在するため、鍵の解読をより難解なものにすることができる。すなわち、暗号文4に対する第3者の復合が難解なものとなる。

【0012】上記のように生成された鍵暗号文7は、鍵管理人や、企業の経営者などの特定人が例えば、フロッピーディスク（図示せず）などに格納して通常は金庫内に保管しておく。

【0013】次に暗号文4の復合について述べる。鍵暗号文7の復合の説明図である。まず、鍵暗号文7の暗号の解読を行う。この場合には、第2暗号化アルゴリズム5にしたがって前記第2パスワードデータ6により鍵暗号文7の暗号の解読処理8を行うことにより、第1パスワードデータ3を読み出す。

【0014】次いで、この第1パスワードデータ3を鍵として、暗号文4の解読を第1暗号化アルゴリズム2にしたがって行うことにより、平文1を読み出す。このようにして、平文1の復合を行う。つまり、第2パスワードデータ6、第1パスワードデータ3の2重の解読を行って暗号文4の解読を行う。したがって、暗号文を解読するために、第1のパスワードデータを得ようとしても、第1のパスワードデータ3は暗号化され鍵暗号文7として存在する。さらに、鍵暗号文7を解読するために必要な第2のパスワードデータは、特定人固有のデータである。従って、平文1に対するセキュリティは非常に高いものとなる。

【0015】次に、本発明の適用例について図2により説明する。図2は機械Aと機械Bに本発明を適用し、また、機械Aに適用されたシステムを機械Cの複写した場合を示している。図2において、機械A内の符号「2A、4A、5A、7A」で示す部分及び機械B内の符号「2B、4B、5B、7B」で示す部分は、それぞれ図1の符号「2、4、5、7」で示す部分に対応するものである。機械Aに対し、本発明に係わる第1のパスワードデータ2A、第2のパスワードデータ5A、暗号文4A及び鍵暗号文7Aから成るシステムを導入し、また、機械Bに対して、同様に、本発明に係わるシステムを導入する。これにより、各機械において、それぞれ本発明に係わるセキュリティを構築することにより、各機械にはそれぞれ独自のセキュリティが構築されたことになる。いま、機械Aにおいて、暗号文4A、鍵暗号文7A第1暗号化アルゴリズム2A及び第2暗号化アルゴリズム5Aが本発明が導入されていない機械Cに複写された場合を想定する。機械Cでは、暗号文を復合すべく第2の暗号化アルゴリズムのパスワードデータが得られないため、暗号文4Aの解読は不可能となる。一方、本発明に係わるシステムが導入された機械A及び機械Bにおいて、機械Aの暗号文Aが機械Bに複写された場合を想定

する。機械Bのシステムは機械Aと同一システムであるため、暗号文4Aを解読する手順は同一である。しかし、機械Bにおいても、第2のアルゴリズムのパスワードデータが得られないため暗号文4Aの解読は不可能となる。なお、本発明に係わるシステムが挿入された機械に対し、通信等の正規経路を介して暗号文を送信し、暗号文4Aの解読を許可する場合は、送信先の機械に対して第2のアルゴリズムのパスワードデータを供与することにより、暗号文4Aが解読される。

【0016】図2の適用例からも明らかなように、ある所定の機械から暗号文、第1パスワードデータ、暗号化アルゴリズム、鍵暗号文を複製して、別の機械に移行して暗号文を稼働させようとしても、第2パスワードデータが得られない限り、第1パスワードデータを取り出すことができないので、暗号文の解読が不可能である。したがって、暗号文のデータの保護が可能となる。また、正規のユーザによる機械Aから機械Bへの通信データなどに対しては、機械Bが機械Aで使用した第2のパスワードデータを享受することにより、暗号文の解読が可能である。

【0017】なお、前記実施例および前記適用例の説明において、第2のパスワードデータとしては、パソコン自体に割り当てられた固有情報であるシリアルナンバー若しくは特定人に割り当てられた固有情報であるID番号またはそれらを組み合わせた複合データによるパスワードデータでもよい。

【0018】

【発明の効果】以上のように、本発明によれば、所定の

暗号化アルゴリズムを使用して、1人または複数の所定の人に割り当てられた第1パスワードデータにより平文のデータのランダム化処理を行って暗号文を生成し、特定人のみに割り当てられた特定人固有の第2パスワードデータにより第1パスワードデータを所定のアルゴリズムを使用して、少なくとも1回のランダム化処理を行って第1パスワードデータから鍵暗号文を生成するようにしたので、小さなキーワードデータにより、容量の大きいデータの暗号化と高度な個人認識とが可能化となる。また、データの改ざん、不法複製の防止、秘匿性の確保、などを確実に行うことができる。これにともない、製品やプログラムの使用許諾への道を開くことができるとともに、コピープロテクション、管理データの保全など様々なところで応用することができる。

【図面の簡単な説明】

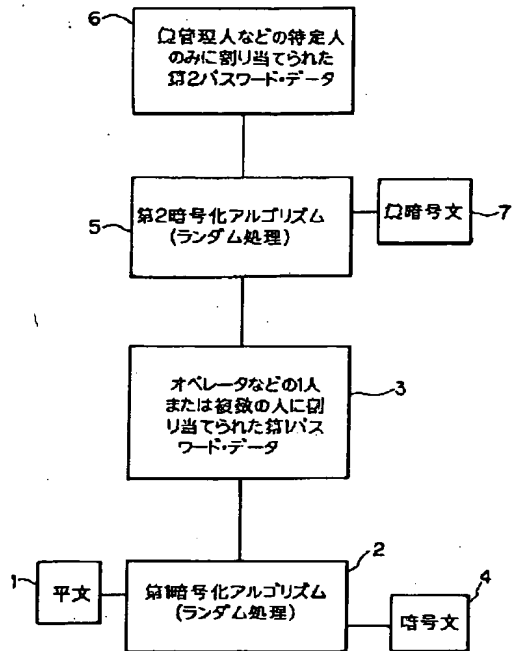
【図1】本発明のセキュリティ構築方法の一実施例の暗号化処理手順を示す説明図である。

【図2】本発明のセキュリティ構築方法の適用例の説明図である。

【符号の説明】

- 1 平文
- 2 第1暗号化アルゴリズム
- 3、3A、3B 第1パスワードデータ
- 4、4A、4B 暗号文
- 5 第2暗号化アルゴリズム
- 6、6A、6B 第2パスワードデータ
- 7、7A、7B 鍵暗号文

【図 1】



【図 2】

